Chief Information Officer's Section
Office of the Governor
State of Utah

December 12, 2001

State Information Security Charter

Authority: This charter and all security policies for the State of Utah will be pursuant to the Governor's Executive Order "To Develop and Implement Policy Promoting Security of State Information and Information Systems", dated December 11, 2001; *Utah Code 63D-1-105, 63A-6-103* and *63-2 Part 2;* and *Utah Administrative Rule R365-4 "*Information Technology Protection," together with other specific security requirements located in agency statutes.

Business need for security: State of Utah executive management has a fiduciary duty to preserve, improve, and account for State information and information systems, which are recognized as critical and important State assets. Management must ensure that information and information systems are properly protected from a variety of threats, including error, fraud, embezzlement, improper disclosure, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, and natural disaster.

Scope of the charter: This charter covers all employees, contractors, part-time and temporary workers, and those employed by others to perform work on State of Utah premises, or granted access to State of Utah information or systems on State computer systems or non-State systems acting as information hosts. Information regarding this charter and its implementation will be made available to all affected staff by the State of Utah manager responsible for the performance of that staff member.

Duties of the staff responsible for various security functions: All employees, contractors, and temporary and part-time workers are responsible for ensuring that State of Utah information assets are used in an authorized manner.

The Chief Information Officer (CIO) is responsible for security policies and for ensuring that appropriate security controls and mechanisms are in existence and in force throughout the State of Utah in keeping with that policy. The CIO will designate an individual to serve as the Chief Information Security Officer (CISO), and that individual will be based in ITS.

The CISO, under the direction of the CIO and the Director of ITS will be responsible for implementing the enterprise security policy and advising state information resource owners and agency level security administrators with regard to the enterprise policy. The CISO is responsible for ensuring that all enterprise authentication and authorization management systems are current and accurate. The CISO will serve as chair of the State Information Security Committee (SISC).

SISC is responsible for assisting the CIO in developing and reviewing State security policies and procedures, reviewing security implementation projects and ensuring that information security practices and policies are appropriately implemented within the Executive branch of government. All executive agencies are entitled to representation.

Information Technology Services (ITS) will ensure that appropriate security controls are in existence and in force throughout the State of Utah. ITS and associated agency level security administrators will implement and enforce enterprise security policies and advise state information resource owners with regard to the policy. Associated agency level security

administrators and managers will further implement and enforce agency specific security policies and ensure such policies do not conflict with enterprise information security policies.

All production application system information must have a designated owner. Application design and development staff will ensure that security policies are effectively and efficiently implemented within all applications that they develop or oversee. Applications will utilize, administer and implement the approved State of Utah security infrastructure, and security policy.

Any employee involved in selecting or purchasing computer system or application software will ensure that the State security policy can be effectively implemented for that system or application prior to its purchase and installation.

In conjunction with the CISO and the agency level security administrator, State of Utah agency management will evaluate all stored information, applications, and information systems to determine the appropriate controls required to protect the information asset on the basis of its criticality to the business, value to the State of Utah, and potential value to external entities consistent with security policy. These evaluations will be documented and reviewed on an annual basis. In addition, ITS, under the direction of the CISO, will conduct and document ongoing reviews of risks to state information and systems and report the results of these reviews at least annually to the Director of ITS and the CIO.

Each agency director will assign one or more agency business managers the responsibility as information resource owners. Information owners are the agency managers and executive management within the State of Utah who bear responsibility for the acquisition, development, updating, and dissemination of State of Utah information processed by production applications. In addition, each agency director will designate an agency level security administrator.

Violation reporting and escalation: Any person covered by this policy is obligated to report apparent violations of this policy to the State of Utah manager to whom they report. If the violation does not appear to be resolved in a timely manner, the person observing the violation will notify the agency security manager or the ITS security manager designated to deal with security violations.

Scope of contingency and disaster recovery: Inability to make use of information assets is as damaging to the State of Utah as destruction of that asset. A written plan for continuing business operations while an information asset is unusable because of a natural or manmade disaster will be documented and tested annually for all information assets identified as critical by the appropriate agency resource owner. ITS will assist in the creation of such plans and also with agency testing processes.

Legal or regulatory requirements: The State of Utah will comply with the security guidelines promulgated by the National Computer Security Center, the arm of the U.S. National Security Agency that defines criteria for trusted computer products and will maintain C-2 criteria for trusted computer products in State of Utah data centers. Compliance with other standards such as Trusted Computer Systems Evaluation Criteria (TCSEC), and DOD Standard 5200.28 will also be maintained, based upon specific Federal agency security requirements.

References:

Interim Date: January 8, 2001
Revision Date: December 12, 2001
Sponsoring Organization(s): CIO, and the State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: January 18, 2001, December 20, 2001
Author(s): Robert Woolley and SISC Committee Members